Department of Homeland Security Daily Open Source Infrastructure Report for 23 February 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports two planes came within a few hundred feet of each other on Friday, February 17, when a controller at Los Angeles International Airport mistakenly cleared three planes for the same runway. (See item 13)
- The Federal Aviation Administration is investigating what caused two jets to collide as they prepared for takeoff at Newark Liberty International Airport on Monday, February 20. (See item 14)
- The World Health Organization reports thirteen countries have reported their first cases of H5N1 infection in birds since the beginning of February. (See item 29)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 22, Rutland Herald (VT)* — **Lightning strike wrecks Searsburg turbine blade.** A 66−foot blade on one of the 11 wind turbines on Mount Waldo in Searsburg, VT broke in half last Friday, February 18, after it was struck by lightning during a fierce windstorm. Green Mountain Power spokesperson Dorothy Schnure said that the wind facility was shut down at the time of the lightning strike because of the high winds. It was the third time the Searsburg

turbines had been struck by lightning since the facility started operating nine years ago, and the second time the turbine damaged Friday had been struck. The incident prompted the chairman of the Londonderry Planning Commission to call for a state investigation. That panel is reviewing plans for the state's largest commercial wind facility on Glebe Mountain. Peter Pagnucco of Londonderry said while Searsburg was relatively remote and posed little danger to the public from breaking turbine blades, that wasn't the case for the Londonderry−Windham facility; skiers at Magic Mountain Ski Area would only be 400 feet from one of the proposed turbines on Glebe Mountain. Since the first lightning strike, a couple of $80,000 replacement blades have been kept on site, but replacement and repairs must wait until there is no wind.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20060222/NEWS/602220377/1003/NEWS02

2. *February 22, Reuters* — **Sierra Pacific reports explosion at Nevada power plant.** Nevada Power Co. said there was an explosion at the 580−megawatt (MW) block 2 at the Chuck Lenzie natural gas−fired power station in Nevada on Monday, February 13. In a filing with the U.S. Securities and Exchange Commission earlier this week, the company said the explosion likely resulted from a build−up of gas during the testing of one of the heat recovery steam generators. The company expected the block to enter service in time for the peak summer air conditioning season. Nevada Power expects the project's engineering and construction contractor, Fluor Corp., to report on the damage and any effect on the planned startup by the end of next week. The explosion did not cause any injuries but damaged the heat recovery steam generators and the surrounding area, the company said. The company also noted the explosion did not damage the adjacent 580 MW block 1, which entered service last month. The 1,160 MW Lenzie combined cycle station is located in the Moapa Valley about 20 miles northeast of Las Vegas, NV. There are four gas−fired combustion turbines, two steam turbines and four heat recovery steam generators at the station.
Source: http://today.reuters.com/business/newsarticle.aspx?type=naturalResources&storyID=nN22295466&imageid=&cap

3. *February 21, Bloomberg* — **New technology for nuclear reactor.** A Chinese group plans to start construction this year of the world's first commercial nuclear power plant using pebble−bed technology, which scientists say can be safer and cheaper than conventional plants. The 200−megawatt reactor will be built in Shandong Province in eastern China. Last year, China began a plan to expand nuclear power capacity almost six fold by 2020 to curb a soaring oil import bill and pollution from coal− fired stations. The pebble−bed project is part of a growing reactor construction program that has made China the world's biggest market for new nuclear power plants. The technology uses kernels of uranium oxycarbide surrounded by carbon and silicon carbide, either in hexagonal shapes or billiard ball−sized pebbles. Eskom Holdings says the safety of the technology comes from the fact that helium, which is used to transfer heat from the core to the power−generating turbines, is chemically inert, so it cannot combine with other chemicals, and it is non−combustible. Because air cannot enter the primary circuit, oxygen cannot get into the high−temperature core to corrode the graphite in the reactor, Eskom says on its Website. Thus, chemical reactions and oxidation, "two of the great dangers in conventional reactors," are sidelined, Eskom said.
Source: http://www.iht.com/articles/2006/02/21/business/chinuke.php

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *February 22, Daily Freeman (NY)* — **Gasoline leak closes New York service area.** The Malden, NY, service area on the Thruway was closed Wednesday, February 22, after two gas station employees reported feeling sick and a suspicious odor shortly after 5 p.m. EST. State police Troop T spokesperson Sgt. Brian Bollard said the entire rest area was closed at 5:40 p.m. EST, and it was determined that the smell was fumes from a gasoline leak underground. "The fumes collected in the gas station kiosk," Bollard said. The two employees were treated at the scene and felt much better after they got back out into the fresh air, he said. Identification of the odor took some time, Bollard said, because when the two employees opened the door to leave the kiosk the wind dissipated the fumes and emergency crews had to wait until more collected in the kiosk before they could test properly. The restaurant was reopened at 9 p.m. EST but the gas station portion of the rest area remains closed.
   Source: http://www.zwire.com/site/news.cfm?newsid=16172443&BRD=1769&PAG=461&dept_id=72585&rfi=6

5. *February 22, Cumberland Times−News (MD)* — **Chemical leak sickens Maryland students.** Nearly 300 Westernport, MD, Elementary School students and staff were evacuated Tuesday, February 21, when a common chemical added for odor detection to natural gas was briefly released from the NewPage Luke Mill. Allegany County Health Officer Dr. Sue Raver said approximately 40 students were sent home from Westernport Elementary and Westmar Middle School with complaints of nausea or respiratory symptoms. Those evacuated were transported to the middle school when gas from the accidental leak entered the elementary school through the heating and ventilation system. Different respiratory complaints, headaches and dizziness warranted assessment and the treatment of four individuals at the elementary school, with several more needing treatment once arriving at the middle school. In a statement prepared and released jointly by the NewPage Corp. and the Allegany County Health Department, the paper mill said a small amount of a colorless gas liquid was released about 8 a.m. EST. That quantity contained less than one percent of Methyl Mercaptan, which Raver explained is "a natural substance released from decaying matter. It's a colorless gas with a smell like rotten cabbage or rotten eggs."
   Source: http://www.times−news.com/articles/2006/02/22/sections/top_s tories/top01.txt

6. *February 21, Associated Press* — **Thousands of gallons of gasoline spilled in Maryland county.** State environmental officials say it may take several years to clean up after a 25,000−gallon gasoline spill from an underground tank in the Jacksonville area of northern Baltimore County, MD. Officials say the leak came from a tank at an ExxonMobil gas station at the intersection of Jarrettsville Pike and Paper Mill Road. The problem began Thursday, February 16, but Maryland Department of the Environment (MDE) officials say authorities were not notified of the leak until Friday, February 17. Since then, they've been monitoring for potentially hazardous vapors and testing utilities and the groundwater for signs of contamination. MDE Secretary Kendl Philbrick says the cause of the leak is still being investigated. She says the state will push Exxon to recover as much of the gasoline as quickly as possible since the leak is in a high−risk groundwater area where many of the residents get their water from underground wells.
   Source: http://www.abc2news.com/news/new−site/06−02−21−gas−spill.sht ml

[Return to top]

Defense Industrial Base Sector

7. *February 22, Defense Ministers & Parliamentary Secretary (Australia)* — **Australian government to improve Army's firepower.** The Australian Government has provided first pass approval for the replacement of their Army's current 105mm and 155mm artillery pieces with new, more capable, artillery systems under a project known as LAND 17. The Australian Defense will now develop the project which invests in artillery systems with longer range, improved precision, and better crew protection. Options for replacing the current towed artillery pieces include a mix of protected self−propelled artillery systems, and lightweight towed artillery systems. As an additional benefit, the project will also examine advanced high precision munitions and a networked command and fire control system. The Australian Defense has been working closely with industry and the Department plans to release an open Request for Tender later this year, to identify companies that can provide artillery systems with the level of capability sought.
   Source: http://www.minister.defence.gov.au/NelsonMintpl.cfm?CurrentI d=5418

8. *February 21, Agence France−Presse* — **Russia's Putin approves creation of Russian aviation giant.** Russian President Vladimir Putin has approved the creation of a new state−controlled aircraft−building group with the aim of consolidating the fragmented Russian industry, the president's office said on Tuesday, February 21. The new group, to be called the Unified Aircraft−Building Corp. (UABC), is to bring together Russian makers of military and civil aircraft and will be at least 75−percent owned by the Russian state. "The proposition of the government to create an aeronautical company consolidated by the Russian Federation and the shareholders of aeronautic companies has been endorsed," said a decree published on the president's Website. Discussions with groups to determine their participation in the company are to take place between now and April 2007. Russian Defense Minister Viktor Khristenko said last year that the Russian aeronautical sector should "increase its production by two and a half times by 2015 to reach $7 billion." The head of EADS Russia, Vadim Vlasov, told Agence France−Presse that the creation of UABC was the first step of an initiative to bring together a number of Russian companies in the sector.
   Source: http://www.defensenews.com/story.php?F=1550672&C=europe

[Return to top]

Banking and Finance Sector

9. *February 22, The Independent (UK)* — **London police arrest banking fraud gang.** Police investigating a suspected banking fraud arrested 13 people on Tuesday, February 22 in a series of early morning raids. The eight men and five women were held during searches of 14 addresses in Ealing, Hayes and Hammersmith, in west London, and Bradford, West Yorkshire, UK. The swoop is part of a City of London Police investigation into a criminal gang suspected of opening bank accounts in false names, using false documents, and then inflicting significant losses on those accounts. Millions in loss is estimated to UK clearing banks and finance

companies as a result of their alleged activities. Detective Sergeant Martin Peters said, "This investigation has focused on the addresses of a group of organized individuals, who have been fraudulently attacking the UK clearing banks by opening bank accounts in false names using false documents."
Source: http://news.independent.co.uk/uk/crime/article347031.ece

10. *February 22, Kyodo News (Asia)* — **Personal info on several thousand convicts leaked onto Internet.** Personal information on about 3,400 convicts has been leaked onto the Internet through a virus−infected personal computer of a prison officer, Japanese Justice Ministry officials said Wednesday, February 22. After investigating the case that came to light earlier this month, the ministry confirmed the leaked information included the names of detainees in prison or detention facilities in the Japanese prefectures of Fukuoka and Shiga who have mostly finished their terms and left, as well as personal information on about 2,300 prison employees, they said. More than 10,000 items of data were leaked onto the Internet after an officer at Kyoto Prison received a CD containing the data from another officer at Kagoshima Prison. The ministry was notified of the leak on February 3. The prison officers have told the Justice Ministry they exchanged information thinking it would just stay between them and would not be leaked outside, the officials said.
Source: http://asia.news.yahoo.com/060222/kyodo/d8fu0p1g0.html

11. *February 21, TechWeb News* — **More than half of business PC users receive at least one phish daily.** More than half of business PC users receive at least one phishing e−mail every day, a UK−based security company said Tuesday, February 21. According to a survey conducted by Sophos of 600 business users, 58 percent reported seeing one or more phishing mails in their inboxes daily. More than one in five −− 22 percent −− receive five or more each day. "The reason phishing e−mails are so prevalent is due to their success rate," said Carole Theriault, senior security consultant at Sophos. Identity theft attempts typically start with an e−mail which purports to be from a trusted source, usually a bank, brokerage house, electronic payment provider, or major e−tailer. That message includes a link to a bogus Website where users are duped into divulging data such as credit card and bank account numbers. Sophos' numbers are similar to those of the Anti−Phishing Working Group, which noted in January that the number of phishing attacks in late 2005 reached an all−time high. Last week, Visa Asia Pacific, the Singapore−based division of Visa International, announced that it had shut down 20 spoofed sites run by phishers on reports from customers that they'd received suspicious messages from the company's payment network.
Source: http://www.techweb.com/wire/security/180205467;jsessionid=GO
SXKBZN1X2EAQSNDBECKH0CJUMEKJVN

12. *February 21, VNUNet* — **Identity theft feeds South Korea's billion−dollar gaming black market.** A plague of identity theft is afflicting South Korea's online gamers, as reported cases soar to almost a quarter of a million. Many of the stolen identities are being used in gaming 'farms' in China as part of a $1 billion a year black market in cash and items from online games, according to local media reports. Online games are hugely popular in highly wired South Korea. More than three million people play Lineage and Lineage 2, the games most affected by the recent spate of identify theft. Lineage developer NCsoft Corporation also operates popular games like City of Heroes and Guild Wars in Europe and the U.S., and will launch Auto Assault later this year. There are no reports that any of these games are affected by the Korean

ID thefts. Although there are cases of existing Lineage accounts being hijacked, the victims in the vast majority of recent cases do not even play the game. Instead, their real−world identities have been used to sign up without their knowledge. NCsoft has set up a Website to help Koreans check whether they are victims.
Source: http://www.vnunet.com/articles/print/2150677

[Return to top]

Transportation and Border Security Sector

13. *February 22, Associated Press* — **Three planes avoid runway crash in Los Angeles.** Two planes came within a few hundred feet of each other on Friday, February 17, when a controller at Los Angeles International Airport mistakenly cleared three planes for the same runway, officials said. "It was pretty close," said Les Dorr, a Federal Aviation Administration spokesperson, said. "We'll be looking to find out what all happened, and how we can prevent it in the future." Friday's episode began when the controller directed a departing Skywest turboprop to taxi onto the same runway on which he had cleared a Southwest Airlines jet to land. He also told an Air Canada jet that it could cross the same runway on its way to the terminals. The Skywest pilot saw the incoming Southwest jet and stopped short of the runway. The jet roared past about 275 feet away and 50 feet above the smaller plane. It landed without incident and never got closer than about 5,600 feet to the Air Canada jet, Dorr said. The airport has had one of the worst runway safety violation records in the nation in recent years.
Source: http://www.boston.com/news/nation/articles/2006/02/22/three_planes_avoid_runway_crash_in_la/

14. *February 22, NorthJersey.com* — **Federal Aviation Administration probes jet collision at Newark.** The Federal Aviation Administration (FAA) is investigating what caused two jets to collide as they prepared for takeoff at Newark Liberty International Airport on Monday, February 20. The incident caused long delays but no injuries to more than 250 passengers, Julie King, a spokesperson for Continental Airlines, said Tuesday. The left wing of Miami−bound Flight 589 clipped the tail section of Flight 1002 to Los Angeles as the Boeing 737s were ready to depart, said FAA spokesperson Arlene Murray. The Miami−bound jet struck Flight 1002 as the Los Angeles−bound plane was waiting in a line of departing jets, Murray said. Flight 589 was traveling on an intersecting runway. After the incident, both planes returned to the airport's gates and were taken out of service for repair, Murray said. Murray said the FAA likely will issue a report on the incident by the end of the week. Since 2000, at least seven incidents in which planes have clipped or collided with other planes or objects have occurred on the ground at Newark Liberty, the region's second−busiest airport, with more than 400,000 flights last year.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXk2MDgmZmdiZWw3Zjd2cWVlRUV5eTY4ODQyNjcmeXJpcnk3ZjcxN2Y3dnFlZUVFeXkz

15. *February 22, Houston Chronicle* — **Security breach slows Bush Intercontinental.** Federal authorities shut down Terminal B of Houston's Bush Intercontinental Airport for about an hour and a half on Wednesday, February 22, after a passenger breached a security checkpoint. Houston Airport System spokesperson Richard Fernandez said the woman ran past the checkpoint and was "lost in the crowd" before she could be stopped. The terminal reopened

after the woman was found, but she and numerous other passengers had to be re−screened, said Transportation Security Administration (TSA) spokesperson Andrea McCauley. McCauley said the woman, whose name was not released, had passed properly through the checkpoint, where the metal detectors and TSA screeners are stationed, and into the "sterile" area restricted for passengers with tickets. Later, she walked back into the public area through an exit lane for arriving passengers, then re−entered the sterile area without going through the checkpoint again.
Source: http://www.chron.com/disp/story.mpl/metropolitan/3677762.htm l

16. *February 22, Associated Press* — **Alaska Airlines flight returns after masks deploy.** An Alaska Airlines flight returned to Portland International Airport Tuesday morning, February 21, after the cabin's oxygen masks dropped, 15 minutes into a flight to Denver. There were no injuries and the 69 passengers were placed on other flights to Colorado, said Amanda Tobin, an Alaska Airlines spokesperson. Alaska Airlines has had three similar problems in the last two months. The incidents involved three different types of aircraft and Tobin said the problems don't appear to be connected. On Saturday, February 18, a flight bound for Seattle had to turn around and make an emergency landing at Washington Dulles International Airport after the aircraft did not pressurize properly. Tobin said a door on the Boeing 737−700 was not fully latched. On Valentine's Day, a jet bound for Denver returned to Seattle because of a pressurization problem. Five passengers were treated for ear and sinus pain. The Boeing 737−400, the same type of plane involved in Tuesday's incident, turned around after a warning alarm sounded in the cockpit, indicating a malfunction in the plane's automatic pressurization system, the airline said.
Source: http://www.usatoday.com/travel/flights/2006−02−22−oxygen−dep loys_x.htm

[Return to top]

Postal and Shipping Sector

17. *February 22, DMNews* — **FedEx and Austrade launch initiative to promote exports.** FedEx Express, a subsidiary of FedEx Corp., and the Australian Trade Commission, Austrade, have signed a two−year alliance agreement to expand trade between Australia and the United States. The agreement uses the expertise of both FedEx and Austrade to make expert resources available and connect Australian and U.S. businesses that wish to import and export. The alliance calls for FedEx to promote to its customers the benefits of Austrade's worldwide export assistance network of 100 locations in more than 50 countries, including 18 cities within the United States. The alliance fits within the FedEx international growth strategy, which includes strengthening Australia−U.S. export volume, according to Michael Ducker, executive vice president, International for FedEx Express.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3579 9

[Return to top]

Agriculture Sector

18.

February 22, Agricultural Research Service — **Learning to grow better nursery plants.** A new monitoring system developed by Agricultural Research Service (ARS) scientists in Ohio is teaching researchers and nursery growers how to grow better trees and horticultural plants using more precise, efficient, and safe applications of water, nutrients and pesticides. The system is the brainchild of a team assembled over the past three years by Charles Krause, research leader and plant pathologist in the ARS Application Technology Research Unit at Wooster. Although the lessons learned in the research are still experimental, they're already being adopted so rapidly by nursery operators that some in the industry expect the ARS monitoring system to be commercialized within the next few years. Nursery managers have reduced water use by 40 percent or more by applying these lessons. The system monitors plant needs year−round, currently using 30 sensors for each of three sets of 50 trees. Tests are being done on Red Sunset maple, redbud, and Chanticleer pear trees. The sensors and a weather station linked to computer data loggers take readings −− every minute, 24 hours a day, during the growing season −− of measurements such as soil temperature and moisture.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Food Sector

19. *February 22, Lab Technologist* — **Portable nano and micro sensors developed for food safety.** A European Union funded research project has developed micro and nanotechnology portable devices to detect toxins, pathogens, and chemicals in foodstuffs on the spot. The development means food samples would no longer have to be sent to a laboratory for tests −− a comparatively lengthy and costly procedure −− but could be analyzed for safety and quality at the farm, slaughter house, during transport, or in a processing or packaging plant, the project's researchers say. Currently the detection of bacteria or pesticides in different foodstuffs is only possible by sending samples to a laboratory and waiting hours or days for the results. A portable device would not only accelerate the testing procedure, but would allow more tests to be carried out on more produce samples, increasing the overall safety of the food. The project is developing tiny biomechanical and microelectronic sensors that can be used to screen for virtually any pathogen or toxin in any produce.
Source: http://www.labtechnologist.com/news/ng.asp?n=65976−nanotechnology−food−safety−sensor

20. *February 22, Korea Times* — **Baby formula recalled.** U.S. baby food maker Mead Johnson & Company decided to voluntarily recall some of its powdered milk products circulating in South Korea after they were found to contain metal−like substances, the company said Tuesday, February 21. An internal investigation is under way to determine what the substances are and whether they are harmful to humans, the company said. South Korea's Ministry of Agriculture and Forestry is also conducting tests on the products after being notified by the Korea Food and Drug Administration that foreign objects were found in them.
Source: http://times.hankooki.com/lpage/biz/200602/kt2006022223020011910.htm

21. *February 22, University of Arkansas, Food Safety Consortium* — **In the processing plant, pathogens learn to survive the stress.** There's no doubt that irradiation is effective at eliminating pathogenic bacteria from meat in a processing plant before it's shipped out. But

irradiation can be less effective if plant personnel don’t use it in sufficient doses and if they don’t account for the strength of the bacteria they’re trying to kill. The problem arises because pathogenic bacteria can develop resistance to food processing methods as they grow in a processing plant’s environment, explained Aubrey Mendonca, an Iowa State University food science researcher. They can adapt to the stressful conditions they encounter and become hardy enough to survive a dose of irradiation if the dose isn’t strong enough. When food processors determine at what level they will irradiate meat, they often look for the most effective minimum dose. That determination is usually made by relying on studies that show how much irradiation is needed to kill pathogens. Mendonca said the flaw in that approach occurs when processors use studies of pathogens that are cultured under optimal growth conditions in a laboratory. The conditions that those microorganisms face in the laboratory are not as stressful as the situations encountered by the bacteria seeking to survive in a processing plant’s environment.
Source: http://www.newswise.com/articles/view/518217/

22. *February 21, Animal and Plant Health Inspection Service* — **Chinese pears back on U.S. market shelves.** The U.S. Department of Agriculture’s Animal and Plant Health Inspection Service (APHIS) Tuesday, February 21, announced that Ya pears from China have passed port of entry inspection, and trade to the U.S. has resumed. APHIS suspended the importation of Ya pears from China in December 2003 after shipments of the fruit were found to be infected with Alternaria sp., an exotic post−harvest disease that poses a significant risk to the U.S. apple and pear industry. Because China has strengthened its phytosanitary measures, APHIS has lifted its suspension to allow, under certain conditions, the importation of Ya pears. Under the regulations, all shipments of Ya pears destined to the U.S. from China must be accompanied by a phytosanitary certificate certifying the origin of the product and that the pears are considered free of quarantine pests. In addition, APHIS requires an additional declaration stating that the commodity has been grown in accordance with regulations that require the pears to be grown in approved orchards and packed in approved packing houses.
Source: http://www.aphis.usda.gov/newsroom/content/2006/02/chipears. shtml

23. *February 21, U.S. Department of Agriculture* — **Japan opens market to fresh U.S. potatoes.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Tuesday, February 21, announced that Japan will end its decades−old ban on the import of U.S. fresh potatoes. Japan is the largest U.S. export market for frozen potatoes, with purchases of over $164 million in 2004. The decision will apply to potatoes shipped between February and June, which will be used to produce potato chips. Japan banned potato imports in 1950 due to phytosanitary concerns relating to the potato wart bacteria and the cyst nematode. The decision to conditionally lift the import ban follows a notice from the U.S. that it has eliminated the potato wart bacteria and has contained the cyst nematode to a limited area. After sending experts to the U.S. last summer for inspections, Japan has authorized imports of potatoes from 14 states: Arizona, California, Colorado, Florida, Idaho, Maine, Michigan, Minnesota, New Mexico, North Dakota, Texas, Oregon, Washington, and Wisconsin. Final inspections of U.S. facilities will be required before shipments can begin. Thus far, inspections have been completed in Idaho, Texas, and California and the first shipment from Idaho is expected to arrive in Japan in March.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/02/0050.xml

[Return to top]

Water Sector

24. *February 21, WOI−TV (IA)* — **Store leaked gasoline into day care's water.** The Iowa Department of Natural Resources (DNR) says a convenience store was the source of gasoline that seeped into a day care's water supply this month in western Iowa. The Shelby Mini−Mart is cleaning up the gasoline discovered in a monitoring well and is assessing the extent of the damage. The state is still investigating whether the leak had other sources. On February 9, DNR officials discovered that petroleum had leaked into the day care's water supply through a plastic pipe instead of the copper or cast iron pipe that prevents gasoline seepage. The pipe has been replaced with a copper line.
Source: http://www.woi−tv.com/Global/story.asp?S=4528298&nav=1LFX

[Return to top]

Public Health Sector

25. *February 22, Reuters* — **World Health Organization to fight fever outbreak in Indian Ocean.** The World Health Organization (WHO) on Wednesday, February 22, said it was sending experts to the Indian Ocean region to help control a crippling mosquito−borne disease that has infected thousands across Mauritius, Seychelles, and Reunion. Chikungunya for which there is no known cure or vaccine, has affected more than 100,000 people in the islands off the southeast coast of Africa. WHO said its team was due to arrive in Reunion on Wednesday, February 22, then travel to other affected islands to assess efforts to control the outbreak and set up a regional surveillance system. "... because there's a lot of movement of people between the islands in the region, there is a risk of it spreading," WHO spokesperson Fadela Chaib told Reuters. Around 100,000 cases have been detected on the French island of Reunion, where health officials blamed the death of a 9−year−old on the infection. Seychelles reported more than 1,000 cases of chikungunya earlier this month, but local officials say the number has now declined. Mauritius says 341 people have been inflicted, but health experts say the number could rise when new figures will be released on Friday, February 24.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://www.alertnet.org/thenews/newsdesk/L22736046.htm

26. *February 22, Reuters* — **West Africa works on plan to contain bird flu.** Ministers and experts from across West Africa met on Wednesday, February 22, to draft a plan to contain the bird flu virus as the Food and Agriculture Organization (FAO) warned of a looming regional disaster. The H5N1 bird flu strain confirmed in Nigeria earlier this month has killed 92 people in Asia and the Middle East since 2003 and triggered the culling of millions of domestic fowl. Experts fear that in Africa, where chickens live in millions of homes, the virus could spread rapidly and largely undetected due to a scarcity of health, veterinary, and laboratory services. The meeting aimed to establish an observation network across West Africa to ensure prompt testing of sick poultry. The FAO recommended the Nigerian government prepare for vaccinations that it said would require thousands of veterinarians. The World Organization for Animal Health (OIE) said it was ready to train African lab technicians to test for bird flu to help

improve facilities for massive bird flu screening. "Most laboratories in West Africa are not yet ready to provide services needed, which will be massive ... it is very urgent across the whole of Africa," OIE Director General Bernard Vallat said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/02/22/AR2006022200785.html

27. *February 22, Agence France−Presse* — **First case of H5N1 bird flu in chickens in European Union.** The H5N1 bird flu virus has been detected in two chickens in Austria, marking the first time the virus has appeared in poultry in the European Union. Health ministry spokesperson Danielle Retzek said the poultry infections were "an isolated case" since the animals were in a refuge and not in a chicken farm where poultry are raised for commercial consumption. Two chickens were contaminated in the Noah's Ark animal pound in the southern city of Graz, apparently infected by a swan that was brought there earlier this month, the head of the pound, Herbert Oster, said. Hans Seitinger, agriculture official for the Styria region, told reporters that three ducks from Noah's Ark had also tested positive for H5N1. Oster said 32 fowl had been slaughtered and sent for testing at an Austrian laboratory, with further results expected. Oster said the swan was brought to Noah's Ark uninjured and apparently healthy on February 10 after it had been found lost in a canal in Mellach near the area where Austria's first cases of infected swans were found earlier this month.
Source: http://news.yahoo.com/s/afp/20060222/hl_afp/healthflueuaustria_060222125803;_ylt=AkzSSCOvxWZdS_A8D6BZ4pWJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

28. *February 22, BBC* — **India seals off town.** Officials in India's Maharashtra state have begun sealing off an entire town where the H5N1 strain of bird flu has been discovered. No one will be allowed in or out of Navapur, which has a population of nearly 30,000, or 19 nearby villages. The measures come after reports that blood samples from people in hospital have tested positive for bird flu. Health Ministry officials say tests on 90 of 95 people for bird flu have proved negative. The other five samples, taken from 12 people who have been quarantined with flu−like symptoms in Maharashtra, are being tested further. Results are expected on Thursday, February 23. "We do not rule out the possibility of humans being affected, and it is a distinct possibility," Health Secretary PK Hota told reporters. Teams of health workers have killed hundreds of thousands of birds around the town of Navapur.
Source: http://news.bbc.co.uk/1/hi/world/south_asia/4739800.stm

29. *February 21, World Health Organization* — **Avian influenza: spread of the virus to new countries.** Thirteen countries have reported their first cases of H5N1 infection in birds since the beginning of February. The 13 countries, listed in order of reporting are: Iraq, Nigeria, Azerbaijan, Bulgaria, Greece, Italy, Slovenia, Iran, Austria, Germany, Egypt, India, and France. On February 20, Malaysia reported a fresh outbreak in poultry after having been considered free of the disease for more than a year. Most European countries with good veterinary surveillance have detected the virus in a small number of wild birds only, with no evidence to date of spread to domestic birds. In Azerbaijan, detection of the virus has coincided with die−offs of domestic birds. In Egypt, outbreaks in domestic poultry have now been confirmed in 10 governorates; deaths have also been reported in exotic zoo birds. In Iraq, presence of the virus in birds was found only after the country confirmed its first human case. In Nigeria, as in India, the first cases were detected in large commercial farms, where the disease is highly

visible and outbreaks are difficult to miss. Apart from Iraq, none of the countries newly affected during February has reported human cases. Iraq has reported two human cases, both of which were fatal.
Source: http://www.who.int/csr/don/2006_02_21b/en/index.html

30. *February 21, New York Times* — **Discovering what works on anthrax.** Early treatment in the 2001 anthrax attacks could have cut the death rate in half, according to a systematic review of the treatment, progression, and mortality of anthrax cases since 1900. For the five victims who died in the attacks, the average time from exposure to antibiotic treatment was almost four and a half days. Researchers found that treatment was rarely successful if it was delayed that long. Antibiotics and draining of fluid from the chest are the best approaches, they said, but even sophisticated intensive care techniques will not work unless multiple antibiotics are started very quickly, preferably even before the symptoms appear. In the 2001 cases, 10 of the 11 victims took two or more antibiotics, and eight of them had repeated procedures to drain fluid from their chests. "There was one who received only one antibiotic and he rapidly died," Jon−Erik Holty, the study's lead author, said. Another victim who did not have the fluid draining procedure died as well. In anthrax cases reviewed by the researchers that occurred before 2001, half the patients received no treatment. Of those, all but one died. All the other patients who survived, whether from the 2001 attacks or in earlier cases, had taken more than one antibiotic.
Source: http://www.nytimes.com/2006/02/21/health/21anth.html?_r=1&or ef=slogin

[Return to top]

Government Sector

31. *February 21, Government Accountability Office* — **GAO−06−290: Architect of the Capitol: Management Challenges Remain (Report).** The Architect of the Capitol (AOC) is responsible for the maintenance, renovation, and new construction of the Capitol Hill complex, which comprises more than three−dozen facilities and consists of nine jurisdictions, such as the U.S. Capitol and the Senate and House Office Buildings. In 2005 and 2006, the Government Accountability Office (GAO) briefed Congress on AOC’s recent progress in implementing GAO’s recommendations and on issues related to AOC’s project and facilities management. This report summarizes GAO’s (1) assessment of AOC’s progress in implementing previous GAO recommendations and in improving project and facilities management and (2) delineation of remaining management challenges. These issues affect a wide range of AOC operations. For example, communication with congressional stakeholders is essential to establish and clarify service and expectation levels. Internal controls, such as a reliable cost accounting system, sound procurement practices, and a comprehensive information security program, are necessary to, respectively, improve project and facilities management, strengthen the integrity of AOC’s procurement processes, and effectively safeguard AOC’s data and information assets. In commenting on this report, AOC generally agreed with its content.
Highlights: http://www.gao.gov/highlights/d06290high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−290

[Return to top]

Emergency Services Sector

32. *February 21, Associated Press* — **Congressional panel to conduct earthquake hearing in Missouri.** Beefing up earthquake preparedness along the New Madrid fault is the focus of a congressional field hearing in St. Louis, this week, as lawmakers work to prevent the lapses that occurred during Hurricane Katrina. The hearing Friday, February 24, will address what federal, state and local officials can do prepare for a major earthquake that could hit southeastern Missouri. "Unlike a hurricane, an earthquake cannot be forecast and gives no warning," said Rep. Jo Ann Emerson (R−MO). Emerson will join members of the House Subcommittee on Economic Development, Public Buildings and Emergency Management at the hearing to highlight the shortcomings in current response plans. For example, only one bridge between St. Louis and Memphis, TN, is built to withstand a magnitude 6.0 earthquake despite the region being a crossroads of interstate highways, river, rail and pipeline transportation, Emerson said. Most of the communications equipment available to first responders could be knocked out if telephone lines or cell phone towers are damaged, she said, while medical equipment and many emergency response vehicles are stored in buildings that can't withstand a major quake.
Source: http://www.montereyherald.com/mld/montereyherald/news/politi cs/13927029.htm

33. *February 21, Contra Costa Times (CA)* — **California county wins approval for updated emergency response plan.** Contra Costa County, CA's, updated emergency response plan won unanimous approval from the board of supervisors last week. The county's Office of Emergency Services worked on the update for much of last year before bringing it before the board. It replaces the plan the board approved in 1996. "A lot has changed since 9−11, and there are more known issues regarding industrial (disasters) as well as levees," said Board President John Gioia. The new plan consists of four parts. The first provides general information, including how the county's departments are organized to function together during a disaster and how the county fits into city, state and federal emergency structures. The following two sections deal with short−term and long−term emergency response plans. The last section details recovery operations, including public assistance and individual assistance programs. The plan breaks down possible emergencies into three categories: natural hazards, technological hazards, and domestic security threats. The update also lays out a "hazard summary" for the entire county that identifies specific threats to different regions. For example, the plan says flooding due to levee failure is the primary threat to East County and West County is threatened by the Hayward Fault.
Source: http://www.contracostatimes.com/mld/cctimes/news/politics/13 923218.htm

34. *February 21, News Guard (OR)* — **Emergency radio signals in Oregon city to receive upgrade.** Steps to improve radio communications for the police and public works departments in Lincoln City, OR, are moving forward. City Manager David Hawker said the city is working to purchase radio equipment for the project. This includes buying repeaters, antenna parts and other needed components. The total cost is estimated to be $105,000. "It's a total replacement of our police and public works repeater system," Hawker said. Improved radio communications are needed because Lincoln City contains a lot of rolling hills, so radio communications can sometimes be fuzzy and hard to hear. This is especially true in the north and south sides of town, Hawker said.
Source: http://www.thenewsguard.com/news/story.cfm?story_no=4153

35. *February 21, Gainesville Sun (FL)* — **Failure halts 911 computer dispatch.** An official with Gainesville, FL, Regional Utilities (GRU) blamed a backup system for malfunctioning and shutting down the Alachua County communications center's ability to dispatch officers using computers for about 20 minutes Monday morning, February 20. Luckily, Alachua County Sheriff's Office spokesperson Keith Faulk said, "There weren't any priority calls that didn't get assistance. Sheriff's Office spokesperson Sgt. Keith Faulk said 911 calls were still coming into the center. But calls couldn't be dispatched to officers via computers, which dispatchers normally use. Instead, dispatchers had to rely on a backup radio system with officers calling in using cell phones. An "uninterrupted power supply" system, meant to keep the communications system operating in case of power outages, failed and halted computer dispatching for about 20 minutes, according to the Sheriff's Office and the director of GRU's communications division. "It's designed not to fail, but it did and we have restored the system," said Ted Kellermann, director of GRU, Monday afternoon. Kellermann said technicians don't know what caused the backup system to fail.
Source: http://www.gainesville.com/apps/pbcs.dll/article?AID=/20060221/LOCAL/60221004/1078/news

[Return to top]

Information Technology and Telecommunications Sector

36. *February 22, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−053A: Apple Mac OS X Safari Command Execution Vulnerability.** A file type determination vulnerability in Apple Safari could allow a remote attacker to execute arbitrary commands on a vulnerable system. Apple Safari is a Web browser that comes with Apple Mac OS X. The default configuration of Safari allows it to automatically "Open 'safe' files after downloading." Due to this default configuration and inconsistencies in how Safari and OS X determine which files are "safe," Safari may execute arbitrary shell commands as the result of viewing a specially crafted Webpage. Systems affected: Apple Safari running on Mac OS X. Impact: A remote, unauthenticated attacker could execute arbitrary commands with the privileges of the user running Safari. If the user is logged on with administrative privileges, the attacker could take complete control of an affected system.
Solution: Since there is no known patch for this issue at this time, US−CERT is recommending a workaround.
Workaround: Disable "Open 'safe' files after downloading". Disable the option to "Open 'safe' files after downloading," as specified in the document "Securing Your Web Browser": http://www.us−cert.gov/reading_room/securing_browser/#sgener al.
Source: http://www.uscert.gov/cas/techalerts/TA06−053A.html

37. *February 21, Security Tracker* — **Tar on Red Hat Enterprise Linux lets remote users write files.** A vulnerability was reported in Tar on Red Hat Enterprise Linux. A remote user can cause files to be written to the target user's system. Analysis: The original vulnerability was a path traversal flaw in the extraction of GNU tar archives. A remote user can create a specially crafted archive that, when extracted by the target user, will write arbitrary files with the privileges of the target user. Solution: Red Hat has issued fixes for this vulnerability. See source for details.
Source: http://securitytracker.com/alerts/2006/Feb/1015655.html

38. *February 21, Security Tracker* — **IBM Tivoli Directory Server zero−byte write error lets remote users deny service.** A vulnerability was reported in IBM Tivoli Directory Server. A remote user can cause denial−of−service conditions. Analysis: A remote user can send a specially crafted request to cause the target service to write to a zero byte length buffer and crash. The flaw can be triggered with the following command using the ProtoVer Sample LDAP test suite (http://www.gleg.net/protover_ldap_sample.shtml): ./run.py localhost 389 2532 1. Vulnerable products: Versions: 4.1, 5.1, 5.2, 6.0. Solution: No solution was available at the time of this entry. IBM has developed a fix which will be available within approximately one week after testing is completed.
The vendor's advisory is available at:
http://www−1.ibm.com/support/docview.wss?uid=swg21230820
Source: http://securitytracker.com/alerts/2006/Feb/1015653.html

39. *February 21, Security Focus* — **Linux kernel stack fault exceptions unspecified local denial−of−service vulnerability.** Linux kernel is reported prone to an unspecified local denial−of−service vulnerability. Analysis: It was reported that this issue arises when a local user triggers stack fault exceptions. A local attacker may exploit this issue to carry out a denial−of−service attack against a vulnerable computer by crashing the kernel.
A complete list of vulnerable products is available at:
http://www.securityfocus.com/bid/14467/info
Solution: For more information and fixes: http://www.securityfocus.com/bid/14467/solution
Source: http://www.securityfocus.com/bid/14467/references

40. *February 21, IDG News Service* — **Impact of worm targeting Mambo CMS low, say researchers.** F−Secure Corp. is warning of a network worm that targets vulnerabilities in the Mambo Content Management System (CMS) and PHP XML−RPC, a library of code for PHP programmers that allows procedures to run between computers with different operating systems. F−Secure calls the worm Mare.D, saying it installs several backdoors on a compromised system. The worm scans random hosts for those running vulnerable installations of the Mambo open source Website content management system or the PHP XML−RPC library. Two of the backdoors −− "cb" and "ping.txt" −− are connectback shell backdoors that are connected to a remote host via port 8080, F−Secure said. The third is controlled by Internet Relay Chat and written in the Perl language. The main component of the worm listens on User Datagram Protocol port 27015 for commands, F−Secure said. Mambo wrote on its Website that it has issued fixes for versions 4.5.3 and 4.5.3h. Those fixes can be downloaded from Mambo's Website. It also recommended that users upgrade their software if they have a version earlier than 4.5.3.
Mambo's Website: http://www.mamboserver.com/
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,108868,00.html

41. *February 21, CNET News* — **Microsoft and Kaspersky Lab have recovered from error causing significant e−mail troubles.** Microsoft and Kaspersky Lab have recovered from an error that caused significant e−mail troubles for some users of Microsoft's Antigen e−mail security software. Antigen users started receiving updates for their Kaspersky Lab antivirus engine again on Tuesday, February 21. Microsoft and Kaspersky had put those on hold after a flawed update caused trouble last week, representatives for Microsoft and Kaspersky said

Tuesday. "As far as both parties are concerned, the problems have been addressed and its business as usual," said Steve Orenberg, president of Kaspersky's North American operations. The problems left some people without fully functional e−mail systems for as long as 10 hours. The culprit was a routine update to the Kaspersky antivirus engine, which was distributed early Thursday morning, February 16. Microsoft in the afternoon offered the previous version of the engine for download to solve the problem. While halting the updates for the Kaspersky engine for several days meant that one engine wasn't updated, users were still protected by the other engines and updates.
Source: http://news.com.com/Kaspersky+update+zaps+Microsoft+antivirus/2100−1002_3−6041792.html?tag=cd.top

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:
VU#999708 − Apple Safari may automatically execute arbitrary shell commands
http://www.kb.cert.org/vuls/id/999708

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:
Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser document.
http://www.us−cert.gov/reading_room/securing_browser/#sgener al

Public Exploit Code for Buffer Overflow Vulnerability in Microsoft Windows Media Player Plug−in for Non−IE Browsers
US−CERT is aware of publicly available exploit code for a buffer overflow vulnerability in Windows Media Player plug−in for browsers other than Internet Explorer (IE). For more information can be found in the following US−CERT Vulnerability Note:
VU#692060 − Microsoft Windows Media Player plug−in buffer overflow
http://www.kb.cert.org/vuls/id/692060

US−CERT urges users to apply appropriate updates and review the workarounds

listed in the Microsoft Security Bulletin MS06−006 to mitigate this vulnerability.
http://www.microsoft.com/technet/security/Bulletin/MS06−006. mspx

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 22159 (−−−), 25 (smtp), 8529 (−−−), 139 (netbios−ssn), 54000 (−−−), 29398 (−−−), 6588 (AnalogX) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

42. *February 22, Reuters* — **Unsafe New York dam has residents fearing flood.** Residents in the rural community of Gilboa, 30 miles from the state capital Albany, are fearful that the Gilboa dam might give way and release its 19 billion gallons of water, flooding their town. If the dam should break, an area of upstate New York with nearly 900,000 residents could be submerged under 30 feet of water stretching for 75 miles. Residents have formed the Dam Concerned Citizens Group, which says if the dam breaks it could be the worst man−made disaster ever in New York state. Schools have undertaken evacuations to test how quickly children can be moved to higher ground. The heightened fear of a dam break came after the New York City Department of Environmental Protection (DEP) which owns the 182−foot−tall structure, told the state in October 2005, that the dam did not meet safety standards and could fail in extreme conditions such as massive rainfall. At a recent state hearing, DEP Commissioner Emily Lloyd said the agency has scheduled remedial repairs at Gilboa for this month and long−range restoration will begin in 2008. DEP officials said they would hope to give up to 12 hours of warning were the dam to collapse
Source: http://www.boston.com/news/nation/articles/2006/02/22/worried_about_dam_upstate_ny_residents_fear_floods/

43. *February 19, New York Times* — **Enlisting school bus drivers to keep an eye out for terrorists.** School bus drivers around the country are being trained to watch for potential terrorists, in a program financed by the Department of Homeland Security. Designers of the program, called School Bus Watch, want to turn 600,000 drivers into an army of observers. Such a training program demands strong oversight, said John Rollins, a former senior Homeland Security intelligence official now with the Congressional Research Service. Otherwise, he said, some bus drivers could think of themselves as undercover agents. Most school bus drivers work part time, often to supplement other income. Under the security program, the drivers are not being trained to be police officers. Their role is to report suspicious behavior to dispatchers, who alert the police and funnel tips to a national analysis center. The new effort is part of Highway Watch, a safety program run by the American Trucking Association and financed since 2003 with $50 million in domestic security money. Schools are the kind of target that terrorists want, said Jeffrey Beatty, a security expert, a place where an attack could have huge symbolic impact and lead to many casualties and spectacular images.

Source: http://www.nytimes.com/2006/02/19/national/nationalspecial3/ 19bus.html

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.